IN THE CLAIMS:

. On amended page 12, at line 1, cancel "New Patent Claims" and substitute --**I CLAIM AS MY INVENTION**-- therefor;

Amend the following claims 1 through 3.

1. (Amended) A method [Method] for forming a first commutative checksum [(KP1)] for digital data comprising the steps of: [which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,]

grouping said digital data into a number of data segments by a computer,

forming [a) in which] a first segment checksum [(PSi) is formed] for each said data segment [(Di)],

forming said [b) in which the] first commutative checksum [(KP1) is formed] by a commutative operation [(⊕)] on said [the] first segment checksums [(PSi)], and

cryptographically protecting said [c) in which the] first commutative checksum [(KP1) is cryptographically protected] by using a [at least one] cryptographic operation.

2. (Amended) A method [Method] for checking a predetermined cryptographic commutative checksum comprising the steps of: [which is allocated to digital data which are grouped into a number of data segments, by a computer,]

grouping digital data into a number of data segments by a computer,

allocating said predetermined cryptographic checksum to said digital data,

subjecting said [a) in which the] cryptographic commutative checksum

[is subjected] to an inverse cryptographic operation to form a first commutative [cryptographic] checksum [(KP1)],

forming [b) in which] a second segment checksum [(PSj) is formed] for each said data segment [(Dj, j = a .. z)],

forming [c) in which] a second commutative checksum [(KP2) is formed] by a commutative operation [(⊕)] on said [the] second segment checksums [(PSj)], and

checking said [d) in which the] second commutative checksum [(KP2) is checked] for a match with said [the] first commutative checksum [(KP1)].

3. (Amended) A method [Method] for forming and checking a first commutative checksum [(KP1)] for digital data comprising the steps of: [which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,]

grouping said digital data into a number of data segments by a computer,

forming [a) in which] a first segment checksum [(PSi) is formed] for each said data segment [(Di)],

forming said [b)in which the] first commutative checksum [(KP1) is formed] by a commutative operation [(⊕)] on said first [the] segment checksums [(PSi)],

cryptographically protecting said [c) in which the] first commutative checksum [(KP1) is cryptographically protected] by using at least one cryptographic operation, which forms a cryptographic commutative checksum [being formed],

subjecting said [d) in which the] cryptographic commutative checksum [(KP1) is subjected] to an inverse cryptographic operation to form a reconstructed first [reconstructed] cryptographic checksum [(KP1)],

forming [e) in which] a second segment checksum [(PSj) is formed] for

each said data segment [(Dj, j = a .. z)] of said [the] digital data to which said [the] first commutative checksum [(KP1)] is allocated,

forming [f) in which] a second commutative checksum [(KP2) is formed] by a commutative operation [(⊕)] on said [the] second segment checksums [(PSj)], and

checking said [g) in which the] second commutative checksum [(KP2) is checked] for a match with said [the] reconstructed first [reconstructed] commutative checksum (KP1).

Cancel claim 4 and substitute the following claims 21, 22, and 23 therefor.

21. A method according to claim 1, further comprising the step of:

forming said first segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

22. A method according to claim 2, further comprising the step of:

forming said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

23. A method according to claim 3, further comprising the step of:

forming said first segment checksums and said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Cancel claims 5 and 6, and substitute the following claims ~~24~~, ~~25~~, and ~~26~~ therefor.

~~24~~. A method according to claim 1, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

~~25~~. A method according to claim 2, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

~~26~~. A method according to claim 3, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Cancel claim 7 and substitute the following claims ~~27~~, ~~28~~, and ~~29~~ therefor.

~~27~~. A method according to claim 1, wherein:

said commutative operation exhibits the property of associativity.

~~28~~. A method according to claim 2, wherein:

said commutative operation exhibits the property of associativity.

~~29~~. A method according to claim 3, wherein:

said commutative operation exhibits the property of associativity.

Cancel claim 8 and substitute the following claims 30, 31, and 32 therefor.

30. A method according to claim 1, further comprising the step of: protecting said digital data wherein said data segments have no ties to a specific ordering.

31. A method according to claim 2, further comprising the step of: protecting said digital data wherein said data segments have no ties to a specific ordering.

32. A method according to claim 3, further comprising the step of: protecting said digital data wherein said data segments have no ties to a specific ordering.

Cancel claim 9 and substitute the following claims 33, 34, and 35 therefor.

33. A method according to claim 1, further comprising the steps of:

protecting said digital data, and

processing said digital data in accordance with a network management protocol.

34. A method according to claim 2, further comprising the steps of:

protecting said digital data, and

processing said digital data in accordance with a network management protocol.

35. A method according to claim 3, further comprising the steps of:

protecting said digital data, and

processing said digital data in accordance with a network management protocol.

Amend the following claims 10 through 12.

10. (Amended) An arrangement [Arrangement] for forming a first commutative checksum [(KP1)] for digital data which are grouped into a number of data segments [(Di, i = 1 .. n)], said arrangement comprising:

[by means of] an arithmetic and logic unit, [which is arranged in such a manner that]

[a)] a first segment checksum, which [(PSi)] is formed for each said data segment [(Di)],

[b) the first commutative checksum (KP1) is formed by] a commutative operation [(⊕)] which forms said first commutative checksum by operating on said [the] segment checksums [(Psi)], and

[c) the first commutative checksum (KP1) is cryptographically protected by using at least one] a cryptographic operation which cryptographically protects said first commutative checksum.

11. (Amended) An arrangement [Arrangement] for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, said arrangement comprising:

[by means of] an arithmetic and logic unit, [which is arranged in such a manner that]

[a) the cryptographic commutative checksum is subjected to] an inverse cryptographic operation to form a first cryptographic checksum [(KP1)] from a

cryptographic commutative checksum formed by a cryptographic operation,

[b)] a second segment checksum [(Psj)] which is formed for each said data segment [(Dj, j = a .. z)],

[c) a second commutative checksum (KP2) is formed by] a commutative operation [(⊕)] which operates on said [the] second segment checksums [(PSj)] which forms a second commutative checksum, and

[d)] a comparator which checks for a match between said [the] second commutative checksum [(KP2) is checked for a match with the] and said first commutative checksum [(KP1)].

12. (Amended) An arrangement [Arrangement] for forming and checking a first commutative checksum [(KP1)] for digital data which is grouped into a number of data segments [(Di, i = 1 .. n)], said arrangement comprising:

[by means of] an arithmetic and logic unit, [which is arranged in such a manner that]

[a)] a first segment checksum, which [(PSi)] is formed for each said data segment [(Di)],

[b) the first commutative checksum (KP1) is formed by] a commutative operation [(⊕)] which forms said first commutative checksum by operating on said first [the] segment checksums [(Psi)],

[c) the first commutative checksum (KP1) is cryptographically protected by using at least one] a cryptographic operation which cryptographically protects said first commutative checksum, [a cryptographic commutative checksum being formed,]

a cryptographic commutative checksum formed by said cryptographic operation,

[d) the cryptographic commutative checksum is subjected to] an inverse cryptographic operation to form a first cryptographic checksum [(KP1)] from

said cryptographic commutative checksum;

[e)] a second segment checksum [(PSj)] which is formed for each said data segment [(Dj, j = a .. z)] of said [the] digital data to which said [the] first commutative checksum [(KP1)] is allocated,

[f) a second commutative checksum (KP2) is formed by] a commutative operation [(⊕)] which operates on said [the] second segment checksums [(Psj)] which forms a second commutative checksum, and

[g)] a comparator which checks for a match between said [the] second commutative checksum [(KP2) is checked for a match with the] and a reconstructed first [reconstructed] commutative checksum [(KP1)].

Cancel ~~claim~~ 13 and substitute the following claims ~~36~~, ~~37~~, and ~~38~~ therefor.

~~36~~. An arrangement according to claim 10, wherein:

said first segment checksums are formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

~~37~~. An arrangement according to claim 11, wherein:

said second segment checksums are both formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

~~38~~. An arrangement according to claim 12, wherein:

said first segment checksums and said second segment checksums are both formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Cancel claims 14 and 15, and substitute the following claims ~~39~~, ~~40~~, and ~~41~~ therefor.

~~39~~. An arrangement according to claim 10 wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

~~40~~. An arrangement according to claim 11 wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

~~41~~. An arrangement according to claim 12 wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Cancel claim 16 and substitute the following claims ~~42~~, ~~43~~, and ~~44~~ therefor.

~~42~~. An arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

~~43~~. An arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

42
~~44~~. An arrangement according to claim 12 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Cancel claim 17 and substitute the following claims ~~45~~, ~~46~~, and ~~47~~ therefor.

43
~~45~~. An arrangement according to claim 10 wherein:
said digital data are protected, and
said data segments have no ties to a specific ordering.

44
~~46~~. An arrangement according to claim 11 wherein:
said digital data are protected, and
said data segments have no ties to a specific ordering.

45
~~47~~. An arrangement according to claim 12 wherein:
said digital data are protected, and
said data segments have no ties to a specific ordering.

Cancel claim 18 and substitute the following claims ~~48~~, ~~49~~, and ~~50~~ therefor.

41
~~48~~. An arrangement according to claim 10 wherein:
said digital data are protected via an arrangement of said arithmetic and logic unit, and
said digital data are processed in accordance with a network management protocol.